IT Security Risk Management Policy V1.0

This Document was written and prepared by J & E Hall Limited. Its use is **CONFIDENTIAL** and must only be used as an internal document. Written authority from a company Director must be obtained prior to circulating this document to any third party

Document information

Prepared By:	Jamie Lovesey	**Copy No.:**	1
Title:	IT Manager		
Reviewed by:	Jamie Lovesey & Andrew Bowden	**Authorised by:**	Andrew Bowden
Title:	IT Manager/Managing Director	**Title:**	Managing Director
Signed:		**Signed:**	
Date of Issue:	~~8~~	**Review Date:**	2022~~19~~
Reference No.:	Information Security Policy	**Version No.:**	~~1~~
Supersedes:	~~1~~		

Amendment No.	Section No.	Page No.	Paragraph No.	Date	Amended By

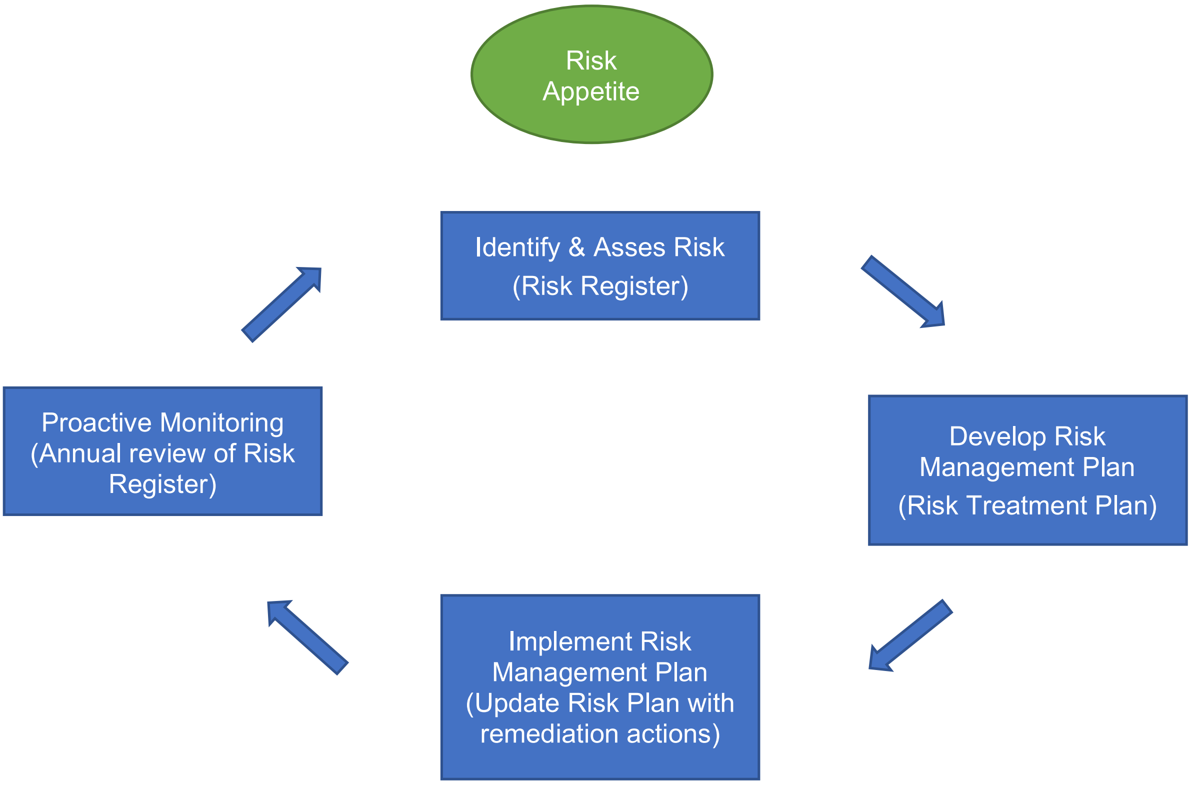
CONTENTS

1. Introduction & Scope

All IT security controls are applied based on a risk assessment using probability verses likelihood to calculate the risk impact. This assessment is used to managed information security controls and ensure that Confidentiality, Integrity and Availability of systems are protected.

We will adopt ISO27005 Information Security Risk management to manage the IT security risks within J&EHall.

2. Risk management lifecycle


Risk Appetite
Identify & Asses Risk (Risk Register)
Develop Risk Management Plan (Risk Treatment Plan)
Implement Risk Management Plan (Update Risk Plan with remediation actions)
Proactive Monitoring (Annual review of Risk Register)

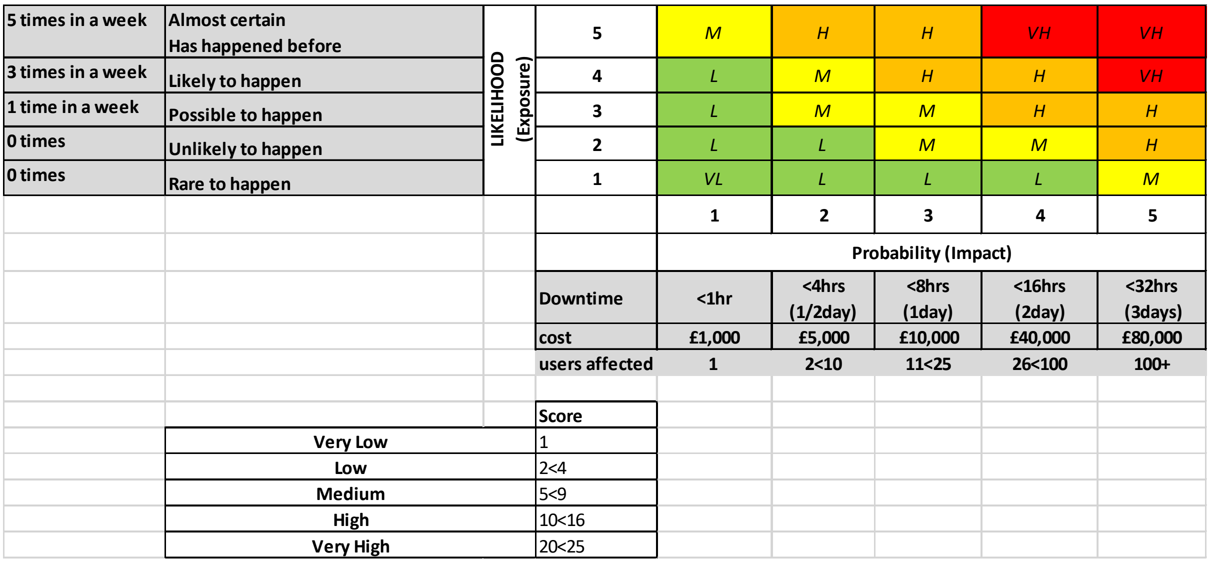
2.1. Document controls

The risk register is the main document and will list all known IT security risks, each risk will be identifiable by an individual reference number. A risk treatment plan will be created for any risks above the risk appetite.

The risk treatment plan must use the same identifiable reference from the risk register that it is creating remediating actions for, it is imperative that these correlate for auditing and tracking purposes.

2.2. Risk Scoring methodology (appetite)

We will be using the following risk matrix to calculate our risks. We will use semi quantitative analysis, where on occasions some form of values will be able to be used. We are using a 5x5 matrix as anything smaller would be too constrained and vague and would be detrimental, meaning most risks would end up in the Low risk category resulting in incorrect risk reading against appetite and no action being taken.

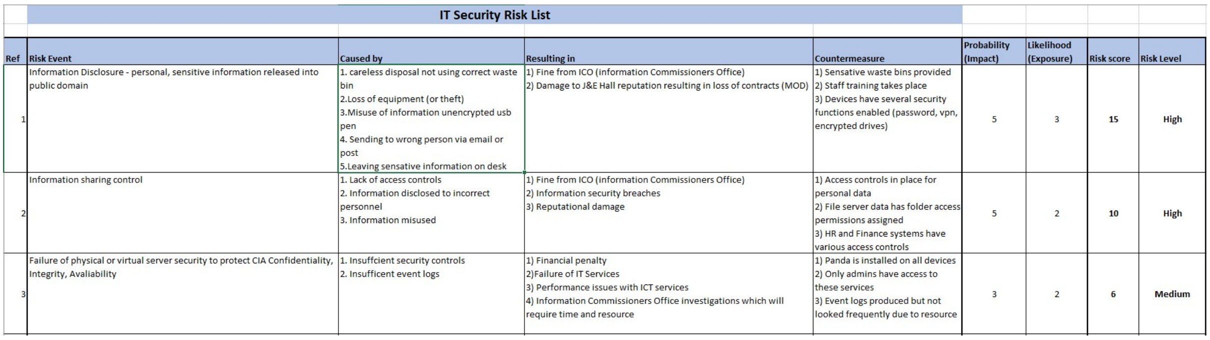


5 times in a week	Almost certain Has happened before	LIKELIHOOD (Exposure)	5	*M*	*H*	*H*	*VH*	*VH*
3 times in a week	Likely to happen		4	*L*	*M*	*H*	*H*	*VH*
1 time in a week	Possible to happen		3	*L*	*M*	*M*	*H*	*H*
0 times	Unlikely to happen		2	*L*	*L*	*M*	*M*	*H*
0 times	Rare to happen		1	*VL*	*L*	*L*	*L*	*M*
				1	**2**	**3**	**4**	**5**
				Probability (Impact)				
			Downtime	**<1hr**	**<4hrs (1/2day)**	**<8hrs (1day)**	**<16hrs (2day)**	**<32hrs (3days)**
			cost	**£1,000**	**£5,000**	**£10,000**	**£40,000**	**£80,000**
			users affected	**1**	**2<10**	**11<25**	**26<100**	**100+**

	Score
Very Low	1
Low	2<4
Medium	5<9
High	10<16
Very High	20<25

3.0 Identify and Assess Risk

To analyze and identify IT security risks we will list known risks in a risk register. The risk register will provide a score and risk level, depending on the risk level depends on remediation options. This will assist with the creation our risk treatment plan.



IT Security Risk List

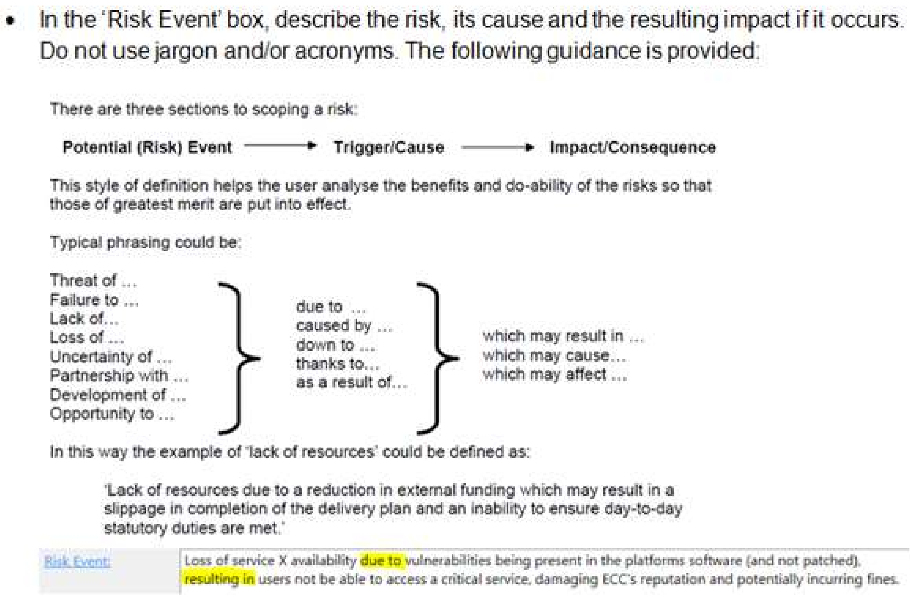
Ref	Risk Event	Caused by	Resulting in	Countermeasure	Probability (Impact)	Likelihood (Exposure)	Risk score	Risk Level
1	Information Disclosure - personal, sensitive information released into public domain	1. careless disposal not using correct waste bin 2.Loss of equipment (or theft) 3.Misuse of information unencrypted usb pen 4. Sending to wrong person via email or post 5.Leaving sensative information on desk	1) Fine from ICO (information Commissioners Office) 2) Damage to J&E Hall reputation resulting in loss of contracts (MOD)	1) Sensative waste bins provided 2) Staff training takes place 3) Devices have several security functions enabled (password, vpn, encrypted drives)	5	3	**15**	**High**
2	Information sharing control	1. Lack of access controls 2. Information disclosed to incorrect personnel 3. Information misused	1) Fine from ICO (information Commissioners Office) 2) Information security breaches 3) Reputational damage	1) Access controls in place for personal data 2) File server data has folder access permissions assigned 3) HR and Finance systems have various access controls	5	2	**10**	**High**
3	Failure of physical or virtual server security to protect CIA Confidentiality, Integrity, Avaliability	1. Insuffcient security controls 2. Insufficent event logs	1) Financial penalty 2)Failure of IT Services 3) Performance issues with ICT services 4) Information Commissioners Office investigations which will require time and resource	1) Panda is installed on all devices 2) Only admins have access to these services 3) Event logs produced but not looked frequently due to resource	3	2	**6**	**Medium**

There are 4 outcomes when calculating risk, we will be using these ;

- Treat (resolve)
- Tolerate (accept)
- Transfer (Share)

- Terminate (Avoid)

When wording the risk assessment form, the following wording will be adopted.



- In the 'Risk Event' box, describe the risk, its cause and the resulting impact if it occurs. Do not use jargon and/or acronyms. The following guidance is provided:

There are three sections to scoping a risk:

Potential (Risk) Event → **Trigger/Cause** → **Impact/Consequence**

This style of definition helps the user analyse the benefits and do-ability of the risks so that those of greatest merit are put into effect.

Typical phrasing could be:

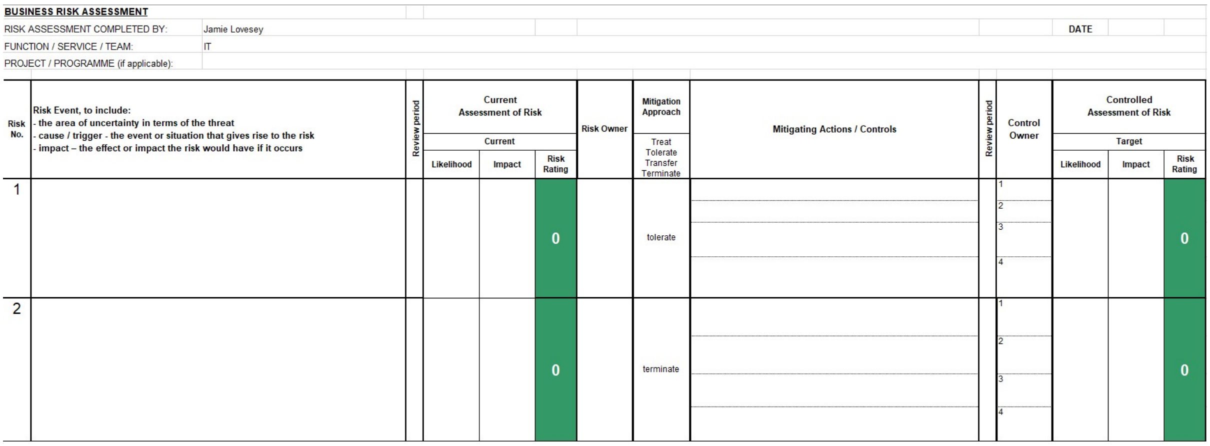
Threat of … Failure to … Lack of… Loss of … Uncertainty of … Partnership with … Development of … Opportunity to …	due to … caused by … down to … thanks to… as a result of…	which may result in … which may cause… which may affect …

In this way the example of 'lack of resources' could be defined as:

> 'Lack of resources due to a reduction in external funding which may result in a slippage in completion of the delivery plan and an inability to ensure day-to-day statutory duties are met.'

Risk Event:	Loss of service X availability due to vulnerabilities being present in the platforms software (and not patched), resulting in users not be able to access a critical service, damaging ECC's reputation and potentially incurring fines.

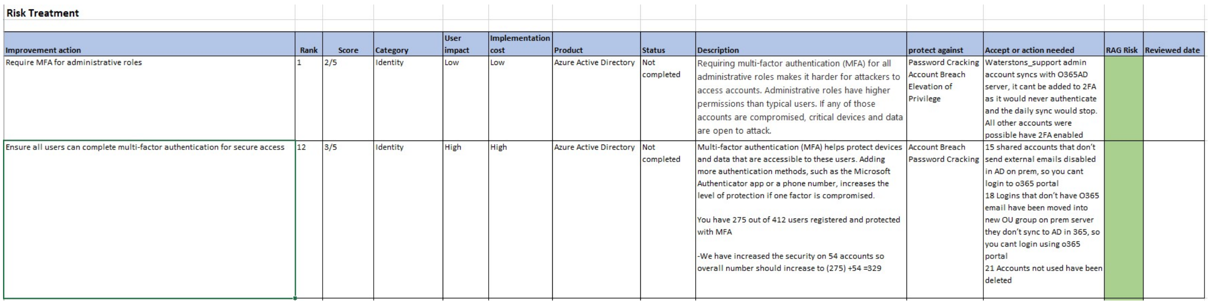
Any new project work or changes to original systems will also be risk assessed before approval. They will be submitted to the IT team by either a new scope of work order or by using a change form. IT will assess the risks using the risk assessment form shown below, and if necessary if the risk is high or very high IT will escalate to senior management approval, IT will then feedback to the requestor.



BUSINESS RISK ASSESSMENT													
RISK ASSESSMENT COMPLETED BY:	Jamie Lovesey										DATE		
FUNCTION / SERVICE / TEAM:	IT												
PROJECT / PROGRAMME (if applicable):													
Risk No.	**Risk Event, to include:** **- the area of uncertainty in terms of the threat** **- cause / trigger - the event or situation that gives rise to the risk** **- impact – the effect or impact the risk would have if it occurs**	**Review period**	**Current Assessment of Risk**			**Risk Owner**	**Mitigation Approach**	**Mitigating Actions / Controls**	**Review period**	**Control Owner**	**Controlled Assessment of Risk**		
			Current				Treat Tolerate Transfer Terminate				**Target**		
			Likelihood	**Impact**	**Risk Rating**						**Likelihood**	**Impact**	**Risk Rating**
1					0		tolerate			1 2 3 4			0
2					0		terminate			1 2 3 4			0

3.1 Develop the risk treatment plan

After analysing the IT security risks and necessary actions the risk treatment plan will be populated accordingly. An example of the Risk Treatment Plan is below. This will be shared with senior management if further authorisation or expense is to be occurred to resolve the risk.



Risk Treatment

Improvement action	Rank	Score	Category	User impact	Implementation cost	Product	Status	Description	protect against	Accept or action needed	RAG Risk	Reviewed date
Require MFA for administrative roles	1	2/5	Identity	Low	Low	Azure Active Directory	Not completed	Requiring multi-factor authentication (MFA) for all administrative roles makes it harder for attackers to access accounts. Administrative roles have higher permissions than typical users. If any of those accounts are compromised, critical devices and data are open to attack.	Password Cracking Account Breach Elevation of Privilege	Waterstons_support admin account syncs with O365AD server, it cant be added to 2FA as it would never authenticate and the daily sync would stop. All other accounts were possible have 2FA enabled	🟩	
Ensure all users can complete multi-factor authentication for secure access	12	3/5	Identity	High	High	Azure Active Directory	Not completed	Multi-factor authentication (MFA) helps protect devices and data that are accessible to these users. Adding more authentication methods, such as the Microsoft Authenticator app or a phone number, increases the level of protection if one factor is compromised. You have 275 out of 412 users registered and protected with MFA -We have increased the security on 54 accounts so overall number should increase to (275) +54 =329	Account Breach Password Cracking	15 shared accounts that don't send external emails disabled in AD on prem, so you cant login to o365 portal 18 Logins that don't have O365 email have been moved into new OU group on prem server they don't sync to AD in 365, so you cant login using o365 portal 21 Accounts not used have been deleted	🟩	

3.2 Implement Risk Management Plan

The Risk Treatment Plan will be used to track the decisions made to reduce the risk exposure, any remediation actions will only take place once authorisation has been approved by either IT or by senior management depending on the risk level. Updates will be provided to necessary personnel. All risks that have been treated will be updated in the Risk Register with their new risk score and status for future review and auditing.

3.3 Proactive monitoring of risk

Senior management and the IT security manager will assess the risk register annually and agree on the risk levels. If risk scores have increased and require action, the original risk assessment form will be reviewed and updated with any possible new remediation actions. The risk treatment plan will be updated to track any remediation actions. Once completed the risk register will be updated to reflect the new risk score.